First Hit Fwd Refs

Previous Doc Next Doc Go to Doc#

Generate Collection Print

L6: Entry 13 of 23

File: USPT

Aug 29, 2000

DOCUMENT-IDENTIFIER: US 6111953 A

TITLE: Method and apparatus for authenticating a document

Detailed Description Text (20):

Another commonly used cryptographic technique, the so-called challenge-response protocol (CRP), may be used to ensure to a recipient that a stamped code is current, i.e., not a copy of a previously used code. This technique would be particularly useful in cases where recurring documents are employed with few if any changes, such as payroll checks or other periodic payments. In the CRP, a requester challenges the device by transmitting a datum to the device, and checking for the same datum in the received response. Thus, reused codes are prevented (or at least detectable) because a reused code would contain a datum corresponding to a previous request/reply pair, rather than the current datum. Those skilled in the art will appreciate that the challenge can use any datum whose value cannot be predicted by the recipient; random numbers happen to be a particularly convenient choice. Alternatively, the device could include a random number generator to generate random numbers internally. In this somewhat weaker version of the CRP, the recipient would not necessarily know that the stamped code was unique, but only that he had not been sent a copy of a code he himself had previously received.

Other Reference Publication (6):

"Photo Checks Reduces Fraud, Approves Checks", NCUA Watch, Feb. 19, 1996 at p. 5.

Previous Doc Next Doc Go to Doc#